ON THE BIRCH AND SWINNERTON-DYER CONJECTURE FOR CM ELLIPTIC CURVES OVER $\mathbb{Q}$

YONGXIONG LI, YU LIU AND YE TIAN

To John Coates for his 70th birthday

Contents

1. Introduction and Main Theorems

For an elliptic curve E over a number field F, we write $L(s, E/F)$ for its complex L-function, $E(F)$ for the Mordell-Weil group of E over F, and $Ш(E/F)$ for its Tate-Shafarevich group. For any prime p, let $Ш(E/F)(p)$ or $Ш(E/\mathbb{Q})[p^\infty]$ denote the p-primary part of $Ш(E/F)$. When $F = \mathbb{Q}$, we shall simply write $L(s, E) = L(s, E/\mathbb{Q})$.

Theorem 1.1. *Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication. Let p be any potentially good ordinary odd prime for E.*

(i) *Assume that $L(s, E)$ has a simple zero at $s = 1$. Then $E(\mathbb{Q})$ has rank one and $Ш(E/\mathbb{Q})$ is finite. Moreover the order of $Ш(E/\mathbb{Q})(p)$ is as predicted by the conjecture of Birch and Swinnerton-Dyer conjecture.*

(ii) *If $E(\mathbb{Q})$ has rank one and $Ш(E/\mathbb{Q})(p)$ is finite, then $L(E, s)$ has a simple zero at $s = 1$.*

Remark. The first part of (i) is the result of Gross-Zagier and Kolyvagin. The remaining part is due to Perrin-Riou for good ordinary primes. In this paper, we deal with odd bad primes which are potentially good ordinary. The result can be easily generalized to abelian varieties over $\mathbb{Q}$ corresponding to a CM modular form with trivial central character.

The following theorem shows that there are infinitely many elliptic curves over $\mathbb{Q}$ of rank one for which the full BSD conjecture hold.

Theorem 1.2. *Let $n \equiv 5 \bmod 8$ be a squarefree positive integer, all of whose prime factors are congruent to 1 modulo 4. Assume that $\mathbb{Q}(\sqrt{-n})$ has no ideal class of order 4. Then the full BSD conjecture holds for the elliptic curve $y^2 = x^3 - n^2x$ over $\mathbb{Q}$. In particular, for any prime $p \equiv 5 \bmod 8$, the full BSD holds for $y^2 = x^3 - p^2x$.*

Sketch of Proof. Consider the Heegner point P constructed using the Gross-Prasad test vector as the below Theorem 1.3. Using an induction argument as in [16] or [17], one can show that P is non-torsion. Thus both the analytic rank and Mordell-Weil rank of $E^{(n)} : y^2 = x^3 - n^2x$ are one.

By Perrion-Riou [12] and Kobayashi [8], we know that the p-part of full BSD holds for all primes $p \nmid 2n$. The 2-part of BSD for $E^{(n)}$ is exactly the statement on 2-divisibility in Theorem 1.3 below by using explicit Gross-Zagier formula in [2] and noting that $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^{(n)}/\mathbb{Q})/\mathrm{Im}(E^{(n)}(\mathbb{Q})_{\mathrm{tor}}) = 1$. By Theorem 1.1, the p-part of BSD also holds for all primes $p|n$, since all primes p with $p \equiv 1 \bmod 4$ are potentially good ordinary primes for $E^{(n)}$. □

To solve the Diophantine equation $y^2 = x^3 - n^2x$ over $\mathbb{Q}$, we define the complex uniformization of $E^{(n)}$ by the following composition.

$$\mathcal{H} \xrightarrow{\pi} \Gamma_0(32)\backslash\mathcal{H} \cup P^1(\mathbb{Q}) = X_0(32) \xrightarrow{f_0} E^{(1)} \xrightarrow{[2-2i]} E^{(1)} \xrightarrow{\iota} E^{(n)},$$

where

- $\mathcal{H} \xrightarrow{\pi} \Gamma_0(32)\backslash(\mathcal{H} \cup P^1(\mathbb{Q})) = X_0(32)(\mathbb{C})$ is the natural quotient,
- $f_0 : X_0(32) \to E^{(1)}$ is a degree 2 morphism over $\mathbb{Q}$ mapping $[\infty]$ to O,
- $[2-2i]$ is the multiplication by $2-2i$ on $E^{(1)}$, where $i(x,y) = (-x, iy)$,
- $\iota : E^{(1)} \xrightarrow{\sim} E^{(n)}$ is the twist isomorphism given by $(x,y) \mapsto \big(-nx,\ (-n)^{3/2}y\big)$.

The following theorem, which is equivalent to the 2-part BSD for $E^{(n)}$ using explicit Gross-Zagier formula in [2], and can be proved exactly as in [16].

Theorem 1.3. *Let $n \equiv 5 \bmod 8$ be a square-free positive integer as in Theorem 1.2. Then the image $P_0 \in E^{(n)}$ of $(4-4\sqrt{-n})^{-1} \in \mathcal{H}$ under the above complex uniformization is defined over the Hilbert class field H of $\mathbb{Q}(\sqrt{-n})$. Moreover the Heegner point $P := \sum_{\sigma \in \mathrm{Gal}(H/\mathbb{Q}(\sqrt{-n}))} P_0^\sigma$ actually belongs to $E^{(n)}(\mathbb{Q})$. Let $\mu(n)$ be the number of prime factors of n. Then $P \in 2^{\mu(n)-1}E^{(n)}(\mathbb{Q}) + E^{(n)}(\mathbb{Q})_{\mathrm{tor}}$ but $P \notin 2^{\mu(n)}E^{(n)}(\mathbb{Q}) + E^{(n)}(\mathbb{Q})_{\mathrm{tor}}$. In particular, P is of infinite order.*

Moreover, the Mordell-Weil group $E^{(n)}(\mathbb{Q})$ is of rank one and the index of its subgroup generated by P and torsion points satisfies

$$\left[E^{(n)}(\mathbb{Q}) : \mathbb{Z}P + E^{(n)}(\mathbb{Q})_{\mathrm{tor}}\right] = 2^{\mu(n)-1} \cdot \sqrt{|\text{Ш}(E/\mathbb{Q})|}.$$

Example For the prime $p = 1493 \equiv 5 \bmod 8$, the Mordell-Weil group $E^{(p)}(\mathbb{Q})$ modulo torsion has a generator

$$\left[\frac{1674371133}{744769},\ -\frac{51224214734700}{642735647}\right],$$

as well that Heegner point (x,y) has coordinates

$$x = \frac{245615354991472149396897545942269693272895149837163013145 3}{2958501182854207571944468687561920064681205358510529},$$
$$y = \frac{121725780668263596873618123810557983972375660184180439465365335709906181098721585260100}{160919109605479862871753246473210772682219745687839109456974711787796868892833}.$$

It follows that $\text{Ш}(E^{(p)}/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^2$.

Let E be an elliptic curve defined over $\mathbb{Q}$, with complex multiplication (= CM in what follows) by an imaginary quadratic field K. Let $p \neq 2$ be a potential good ordinary prime for E. Note that p must split in K, and also p does not divide the number w_K of roots of unity in K.

Assume that $L(s,E)$ has a simple zero at $s=1$. Choose an auxiliary imaginary quadratic field $\mathcal{K}$ such that (i) p is split over $\mathcal{K}$ and (ii) $L(s, E/\mathcal{K})$ still has a simple zero at $s=1$. Let $E^{(\mathcal{K})}$ be the twist of E over $\mathcal{K}$, then $L(1, E^{(\mathcal{K})}) \neq 0$. Let η be the quadratic character associated to the extension $\mathcal{K}/\mathbb{Q}$ and η_K its restriction to K. Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, and put $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. For any finite order character ν of Γ, let $\nu_{\mathcal{K}}$ denote its restriction to $\mathrm{Gal}(K\mathbb{Q}_\infty/K)$. Consider the equality

$$L(s, E \otimes \nu) L(s, E^{(\mathcal{K})} \otimes \nu) = L(s, E_{\mathcal{K}} \otimes \nu_{\mathcal{K}})$$

and its specialization to $s=1$. Let $\mathscr{L}_\varphi, \mathscr{L}_{\varphi\eta_K}$ be the cyclotomic-line restrictions of the two Katz's two variable p-adic L-fucntion corresponding to E and $E^{(\mathcal{K})}$, respectively. Let $\mathscr{L}_{E/\mathcal{K}}$ be the cyclotomic-line restriction of the p-adic Rankin-Selberg L-function for E over $\mathcal{K}$. The ingredients needed to prove the p-part BSD formula of E are the following.

1. Rubin's two variable main conjecture[14] in order to relate the p-part of $\text{Ш}(E/K)$ with $\mathscr{L}'_\varphi(1)$. Note that $\mathrm{ord}_p(|\text{Ш}(E/K)|) = 2\mathrm{ord}_p(|\text{Ш}(E/\mathbb{Q})|)$ for odd p.
2. The complex Gross-Zagier formula [19] and the p-adic Gross-Zagier formula [4], which relate $\mathscr{L}'_{E/\mathcal{K}}(1)$ and $L'(1, E/\mathcal{K}) = L'(1, E/\mathbb{Q}) L(1, E^{(\mathcal{K})}/\mathbb{Q})$.
3. The precise relationship between $\mathscr{L}'_\varphi(1)\mathscr{L}\varphi\eta_K(1)$ and $\mathscr{L}'_{E/\mathcal{K}}(1)$, and also between $\mathscr{L}_{\varphi\eta_K}(1)$ and $L(1, E^{(\mathcal{K})})$. This follows from the above equality of L-series and the interpolation properties of these p-adic L-fucntions.

Suppose that E has bad reduction at p which is potential good for E. Let $\mathfrak{p}$ denote a prime of K above p. There is an elliptic curve E' over K with good reduction at $\mathfrak{p}$. In the process of proof, we need to compare periods, descends etc between E and E'.

Notations. Fix a non-trivial additive character $\psi : \mathbb{Q}_p \longrightarrow \mathbb{C}_p^\times$ with conductor $\mathbb{Z}_p$. For any character $\chi : \mathbb{Q}_p^\times \to \mathbb{C}_p^\times$, say of conductor p^n with $n \geq 0$, we define the root number by

$$\tau(\chi, \psi) = p^{-n} \int_{v_p(t)=-n} \chi^{-1}(t)\psi(t)dt,$$

where dt is the Haar measure on $\mathbb{Q}_p$ such that $\mathrm{Vol}(\mathbb{Z}_p, dt) = 1$. Fix embeddings $\iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $i_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ such that $\iota_p = \iota \circ \iota_\infty$ for an isomorphism $\iota : \mathbb{C} \xrightarrow{\sim} \mathbb{C}_p$. For an elliptic curve E over a number field F and p a potential good prime for E, let $(\ ,\ )_\infty$ and $(\ ,\ )_p$ denote the normalized Néron -Tate height pairing, and the p-adic height pairing with respect to cyclotomic character. Let $P_1, \cdots, P_r \in E(F)$ form a basis for $E(F) \otimes_{\mathbb{Z}} \mathbb{Q}$, define the regulars by

$$R_\infty(E/F) = \frac{\det\left((P_i, P_j)_\infty\right)_{r\times r}}{[E(K) : \sum_i \mathbb{Z}P_i]^2}, \qquad R_p(E/F) = \frac{\det\left((P_i, P_j)_p\right)_{r\times r}}{[E(K) : \sum_i \mathbb{Z}P_i]^2}.$$

For any character χ of $\widehat{K}^\times$, let $\mathfrak{f}_\chi \subset \mathcal{O}_K$ denote its conductor. For an elliptic curve E over K, let $\mathfrak{f}_E$ denote its conductor. For any non-zero integral ideals $\mathfrak{g}$ and $\mathfrak{a}$ of K, let $\mathfrak{g}^{(\mathfrak{a})}$ denote the prime-to-$\mathfrak{a}$ part of $\mathfrak{g}$. Let $\mathbb{D}$ be the completion of the maximal unramified extension of $\mathbb{Z}_p$ and $\mathbb{D}_\chi$ the finite extension of $\mathbb{D}$ generated by the values of χ. Let L_∞/K be an abelian extension whose Galois group $\mathcal{G} = \mathrm{Gal}(L_\infty/K) \cong \Delta \times \Gamma$ with Δ finite and $\Gamma \cong \mathbb{Z}_p^d$. Then for any $\mathbb{D}[[\mathcal{G}]]$-module M and character χ of Δ, put $M_\chi = M \otimes_{\mathbb{D}[[\mathcal{G}]],\chi} \mathbb{D}_\chi[[\Gamma]]$. If $p \nmid |\Delta|$, let M^χ denote its χ-component (as a direct summand).

Acknowledgment. The authors thank John Coates, Henri Darmon and Shouwu Zhang for their encouragement.

2. Katz's p-adic L-function and Cyclotomic p-adic Formula

Let E be an elliptic curve defined over K with CM by K and φ its associated Hecke character. Let $p \nmid w_K$ be a prime split in K and $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$ with $\mathfrak{p}$ induced by ι_p. In particular, $K_\mathfrak{p} = \mathbb{Q}_p$ in $\mathbb{C}_p$ and let $\psi_\mathfrak{p} = \psi_p$ on $K_\mathfrak{p}$ under this identification. Let Ω_E be a $\mathfrak{p}$-minimal period of E over K. Let φ be the associated Hecke character of E and $\varphi_\mathfrak{p}$ its $\mathfrak{p}$-component. Let $\mathfrak{f}_E$ be the conductor of φ.

Let F be an abelian extension over K with Galois group Δ. Assume that $p \nmid |\Delta|$ and denote by $\mathfrak{f}_{F/K}$ the conductor of F. Let $\mathcal{G}$ be the Galois group of the extension $F(E[p^\infty])$ over K. Then $\mathcal{G} \cong \mathcal{G}_{\mathrm{tor}} \times \Gamma_K$ with $\Gamma_K = \mathrm{Gal}(F(E[p^\infty])/F(E[p]))$. Let $\Lambda = \mathbb{Z}_p[[\mathcal{G}]]$. Let U_∞ and C_∞ denote the $\mathbb{Z}_p[[\mathcal{G}]]$-modules formed from the principal local units at the primes above $\mathfrak{p}$, and the closure of the elliptic units for $K(E[p^\infty])$ (see §4 of [14] for the precise definitions.)

Theorem 2.1 (Two variable p-adic L-function)**.** *Let $\mathfrak{g}$ be any prime-to-p non-zero integral ideal of K. Assume that $\mathfrak{f}_E^{(p)}|\mathfrak{g}$. There exists a unique measure $\mu_\mathfrak{g} = \mu_{\mathfrak{g},\mathfrak{p}}$ on the group $\mathcal{G} = \mathrm{Gal}(K(\mathfrak{g}p^\infty)/K)$ such that for any character ρ of $\mathcal{G}$ of type $(1,0)$,*

$$\rho(\mu_\mathfrak{g}) = \frac{\tau(\rho_\mathfrak{p}, \psi_\mathfrak{p})}{\tau(\varphi_\mathfrak{p}, \psi_\mathfrak{p})} \cdot \frac{1 - \rho(\mathfrak{p})p^{-1}}{1 - \overline{\rho(\mathfrak{p})}p^{-1}} \cdot \frac{L^{(\mathfrak{g}p)}(\overline{\rho}, 1)}{\Omega_E}.$$

Here $L^{(\mathfrak{g}p)}(\overline{\rho}, s)$ is the imprimitive L-series of $\overline{\rho}$ with Euler factors at places dividing $\mathfrak{f}p$-removed.

Proof. It follows from the below lemma 2.3 and construction of Katz's two variable p-adic measure, see Theorem 4.14. ∎

Theorem 2.2 (Yager)**.** *For any character χ of $\mathcal{G}_{\mathrm{tor}}$, let $\mathfrak{f} = \mathfrak{f}_\chi^{(p)}$ and $\mu_\mathfrak{f}^\chi := \chi(\mu_\mathfrak{f}) \in \mathbb{D}[[\Gamma_K]]$. Then we have*

$$\mathrm{Char}(U_\infty/C_\infty)_\chi \cdot \mathbb{D}[[\Gamma_K]] = \left(\mu_\mathfrak{f}^\chi\right).$$

Here the measure $\mu_\mathfrak{f}$ is defined as in Theorem 2.1.

Lemma 2.3. *Let E/K be an elliptic curve associated with to a Hecke character φ, p splits in K and write $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$. Let φ_0 be a Hecke character over K unramified at $\mathfrak{p}$. Let Ω_E and Ω_0 be $\mathfrak{p}$-minimal periods of E and φ_0, respectively. Then*

$$\mathrm{ord}_p\left(\frac{\Omega_E \cdot \tau(\varphi_\mathfrak{p}, \psi_p)}{\Omega_0}\right) = 0.$$

Proof. This follows from Stickelberger's theorem on prime ideal decomposition of Gauss sum. In fact, for $\mathfrak{p} \nmid w = w_K$, E has $\mathfrak{p}$-minimal Weierstrass equation of form

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6, \qquad a_2, a_4, a_6 \in K^\times \cap \mathcal{O}_\mathfrak{p}.$$

Note that for $w = 4, 6$, we may-and do- take form $y^2 = x^3 + a_4x$, $y^2 = x^3 + a_6$, respectively. Then there is an elliptic curve E' over K which has good reduction at $\mathfrak{p}$. Let φ' be its associated Hecke character. Then $\epsilon = \varphi\varphi'^{-1} : \mathbb{A}_K^\times/K^\times \to \mathcal{O}_K^\times$ (also viewed as a Galois character via class field theory) is of form $\chi(\sigma) = \sigma(d^{1/w})/d^{1/w}$ for an element $d \in K^\times/K^{\times w}$. Then the twist E' has $\mathfrak{p}$-good model

$$E' : \begin{cases} y^2 = x^3 + da_2x^2 + d^2a_4x + d^3a_6, & \text{if } w = 2, \\ y^2 = x^3 + da_4x, & \text{if } w = 4, \\ y^2 = x^3 + da_6, & \text{if } w = 6. \end{cases}$$

It is easy to check the $\Omega_{E_0} = d^{1/w} \cdot \Omega_E$. Let $\omega : \mathcal{O}_\mathfrak{p}^\times \longrightarrow \mu_w \subset K$ be the character characterized by $\omega(a) \equiv a \bmod \mathfrak{p}$ and let $\chi = \omega^{-(p-1)/w}$. Then $\epsilon_\mathfrak{p} = \chi^k$ for some $k \in \mathbb{Z}/w\mathbb{Z}$. Let $\kappa_\mathfrak{p} \cong \mathbb{F}_p$ be the residue field of $K_\mathfrak{p}$. By Stickelberger's theorem, the Gauss sum $g(\epsilon_\mathfrak{p}, \psi) := -\sum_{a\in\kappa_\mathfrak{p}^\times} \epsilon_\mathfrak{p}(a)\psi(a)$ has $\mathfrak{p}$-valuation $\{k/w\}$. It remains to show that $k = \mathrm{ord}_\mathfrak{p}(d)$. Note that for any $u \in \mathcal{O}_\mathfrak{p}^\times$, $K_\mathfrak{p}(u^{1/w})$ is unramified over $K_\mathfrak{p}$. Thus it is equivalent to show that for any uniformizer π of $K_\mathfrak{p}$,

$$\sigma_u(\pi^{1/w})/\pi^{1/w} \equiv u^{-(p-1)/w} \bmod \mathfrak{p}, \qquad \forall u \in \mathcal{O}_\mathfrak{p}^\times.$$

But it is easy to see this by using local class field theory for formal group associated to $x^p - \pi x$.

For general Hecke character φ_0 over K unramified at $\mathfrak{p}$ (not necessarily K-valued) and Ω_0 its $\mathfrak{p}$-minimal period, it is easy to see that $\mathrm{ord}_\mathfrak{p}(\Omega_0/\Omega_{E_0}) = 0$.

$\square$

Let $\chi_{\mathrm{cyc},K} : \mathcal{G} \to \mathbb{Z}_p^\times$ be the p-adic cyclotomic character defined by the action on p-th power roots of unity. Define

$$\mathscr{L}_{\varphi_E}(s) := \mu_{\mathfrak{f}_E^{(\mathfrak{p})}}(\varphi_E\chi_{\mathrm{cyc},K}^{1-s}), \qquad \forall s \in \mathbb{Z}_p.$$

Rubin's two variable main conjecture implies the following theorem.

Theorem 2.4. *Let E be an elliptic curve defined over K with CM by K and φ its associated Hecke character. Let $p \nmid w_K$ be a prime split in K and $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$. Let r be the $\mathcal{O}_K$-rank of $E(K)$. Assume that $Ш(E/K)(p)$ is finite and the p-adic height pairing of E over K is non-degenerate. Then*

(1) *both $\mathscr{L}_\varphi(s)$ and $\mathscr{L}_{\overline{\varphi}}(s)$ have a zero at $s = 1$ of exact order r.*

(2) *the p-adic BSD conjecture holds for E/K:*

$$\mathrm{ord}_p(|Ш(E/K)|) = \mathrm{ord}_p\left(\frac{\mathscr{L}_\varphi^{(r)}(1)\mathscr{L}_{\overline{\varphi}}^{(r)}(1)}{R_p(E/K)} \cdot \prod_{v|p}\left((1 - \varphi_E(v))\left(1 - \overline{\varphi_E(v)}\right)\right)^{-2}\right)$$

provided the assumption that if $w_K = 4$ or 6 then E has bad reduction at both $\mathfrak{p}$ and $\mathfrak{p}^*$ or good reduction at both $\mathfrak{p}$ and $\mathfrak{p}^*$.

Moreover, if E is defined over $\mathbb{Q}$, then we have

$$\mathrm{ord}_p(|Ш(E/\mathbb{Q})|) = \mathrm{ord}_p\left(\frac{\mathscr{L}_\varphi^{(r)}(1)}{R_p(E/\mathbb{Q})} \cdot \prod_{v|p}\left((1 - \varphi_E(v))\left(1 - \overline{\varphi_E(v)}\right)\right)^{-1}\right).$$

Proof. Let ϵ be a Galois character over K valued in $\mathcal{O}_K^\times$ such that $\varphi' = \varphi\epsilon$ is unramified at both $\mathfrak{p}$ and $\mathfrak{p}^*$. Let E' be the elliptic curve over K as ϵ-twist of E so that φ' as its Hecke character. Then E' has good reduction above p. Let F be the abelian extension over K cut by ϵ, then $[F : K]|w_K$. Moreover, E and E' are isomorphism over F, $E'(F)^{(\epsilon)} \cong E(K)$, and $Ш(E'/F)[p^\infty]^{(\epsilon)} \cong Ш(E/K)[p^\infty]$. Let $F_0 = F(E[p])$ and $\chi : \mathrm{Gal}(F_0)/K) \to \mathcal{O}_\mathfrak{p}^\times$ be the character giving the action on $E[p]$.

Let $F_\infty = F(E[p^\infty])$. Let $M_{\infty,\mathfrak{p}}$ be the maximal p-extension over F_∞ unramified outside $\mathfrak{p}$ and $X_{\infty,\mathfrak{p}} = \mathrm{Gal}(M_{\infty,\mathfrak{p}}/F_\infty)$. Denote by U_∞ and $C_\infty \subset U_\infty$ the $\Lambda = \mathbb{Z}[[\mathrm{Gal}(F_\infty/K)]]$-modules of the principal local units at $\mathfrak{p}$ and elliptic units for the extension F_∞ (defined as in [14], §4). Rubin's two variable main conjecture, together Yager [18], says that

$$\mathrm{Char}_\Lambda(X_{\infty,\mathfrak{p}}^\chi)\mathbb{D}[[\mathrm{Gal}(F_\infty/F_0)]] = \left(\mu^\chi_{f_E^{(p)},\mathfrak{p}}\right),$$

where for an integral ideal $\mathfrak{g}$ of K prime to p, the measure $\mu_{\mathfrak{g}}$ is given as in Theorem 2.1. Let $\mathrm{Sel}(F_\infty, E[\mathfrak{p}^\infty])$ be the $\mathfrak{p}$-Selmer group of E over F_∞ and $\mathrm{Sel}(F_\infty, E[\mathfrak{p}^\infty])^\vee$ its Pontryajin dual. Then $\mathrm{Sel}(F_\infty, E[\mathfrak{p}^\infty])^\vee$ is a finitely generated Λ-torsion module and

$$\mathrm{Char}_\Lambda(\mathrm{Sel}(F_\infty, E[\mathfrak{p}^\infty])^\vee) = \iota_{\mathfrak{p}}\mathrm{Char}(X^\chi_{\infty,\mathfrak{p}}),$$

where $\iota_{\mathfrak{p}} : \Lambda \to \Lambda, \gamma \longrightarrow \kappa_{\mathfrak{p}}(\gamma)\gamma$ for any $\gamma \in \mathrm{Gal}(F_\infty/K)$ and $\kappa_{\mathfrak{p}}$ is the character of $\mathrm{Gal}(F_\infty/K)$ giving the action on $E[\mathfrak{p}^\infty]$. Similarly, we also have that

$$\mathrm{Char}_\Lambda(X^\chi_{\infty,\mathfrak{p}^*})\mathbb{D}[[\mathrm{Gal}(F_\infty/F_0)]] = \left(\mu^\chi_{f_E^{(p)},\mathfrak{p}^*}\right), \qquad \mathrm{Char}_\Lambda(\mathrm{Sel}(F_\infty, E[\mathfrak{p}^{*\infty}])^\vee) = \iota_{\mathfrak{p}^*}\mathrm{Char}(X^\chi_{\infty,\mathfrak{p}^*}).$$

Let F_{cyc} be the cyclotomic $\mathbb{Z}_p$ extension, and $\Lambda_{\mathrm{cyc}} = \mathbb{Z}_p[[\mathrm{Gal}(F_{\mathrm{cyc}}/K)]] \cong \Delta\times\Gamma$ where $\Delta = \mathrm{Gal}(F/K)$ and $\Gamma = \mathrm{Gal}(F_{\mathrm{cyc}}/F)$. Let $\mathrm{Sel}(F_{\mathrm{cyc}}, E[p^\infty])$ denote the p-Selmer group of E over F_{cyc} and then its Pontryagin dual $\mathrm{Sel}(F_{\mathrm{cyc}}, E[p^\infty])^\vee$ is a finitely generated torsion Λ_{cyc}-module. We have

$$\begin{aligned}\mathrm{Sel}(F_{\mathrm{cyc}}, E[p^\infty]) &= \mathrm{Sel}(F_{\mathrm{cyc}}, E[p^\infty]) \oplus \mathrm{Sel}(F_{\mathrm{cyc}}, E[p^{*\infty}])\\ &= \mathrm{Hom}(X_{\infty,\mathfrak{p}}, E[\mathfrak{p}^\infty])^{\mathrm{Gal}(F_\infty/F_{\mathrm{cyc}})} \oplus \mathrm{Hom}(X_{\infty,\mathfrak{p}^*}, E[\mathfrak{p}^{*\infty}])^{\mathrm{Gal}(F_\infty/F_{\mathrm{cyc}})}\end{aligned}$$

Here the second equality is given [10] Proposition (1.3), Theorem (1.6) and Lemma (1.1), the last one is by the same reason as [14] Theorem 12.2. It follows that

$$\mathrm{Char}_{\Lambda_{\mathrm{cyc}}}(\mathrm{Sel}(F_{\mathrm{cyc}}, E[p^\infty])^\vee)\mathbb{D}[[\mathrm{Gal}(F_{\mathrm{cyc}}/F)]] = \left(\iota_{\mathfrak{p}}\mu^\chi_{f_E^{(p)},\mathfrak{p}}\iota_{\mathfrak{p}^*}\mu^\chi_{f_E^{(p)},\mathfrak{p}^*}\right).$$

Denote by χ_{cyc} the cyclotomic character. Let f_E be a generator of $\mathrm{Char}_{\mathbb{Z}_p[[\Gamma]]}(\mathrm{Sel}(F_{\mathrm{cyc}}, E[p^\infty])^\vee)^\Delta$ and define

$$\mathscr{L}(s) = \chi_{\mathrm{cyc}}^{1-s}(f_E), \qquad \forall s \in \mathbb{Z}_p.$$

Then we have $\mathscr{L}(s) = u(s)\mathscr{L}_{\varphi_E}(s)\mathscr{L}_{\overline{\varphi_E}}(s)$ for some function $u(s)$ valued in $\mathbb{D}^\times$.

Note that E over F has good reduction above p. Employing the descend argument as in [15], noting that the "descent diagram" in [15] §7 for E over F is $\Delta = \mathrm{Gal}(F/K)$-equivariant, and taking Δ-invariant part, we have

Proposition 2.5. *Let $r := \mathrm{rank}_{\mathcal{O}_K} E(K)$. Assume that $\text{Ш}(E/K)[p^\infty]$ is finite and p-adic height pairing is non-degenerate on $E(K)$. Then $\mathscr{L}(s)$ has exact vanishing order $2r$ at $s = 1$ and if let $\mathscr{L}^*(1)$ denote its leading coefficient at $s = 1$,*

$$\frac{\mathscr{L}^*(1)}{R_p(E/K)} \sim |\text{Ш}(E/K)| \cdot \left|\prod_{v|p} H^1(\mathrm{Gal}(F(\mu_{p^\infty})/F), E(F(\mu_{p^\infty}) \otimes_K K_v))^\Delta\right|^2.$$

Here for any $a, b \in \mathbb{C}_p^\times$, write $a \sim b$ if $\mathrm{ord}_p(a/b) = 0$.

The follow lemma will complete the proof.

Lemma 2.6. *Let $v_0 = \mathfrak{p}$ or $\mathfrak{p}^*$. Assume that if $w_K = 4$ or 6 then E has bad reduction at both $\mathfrak{p}$ and $\mathfrak{p}^*$ or good reduction at both $\mathfrak{p}$ and $\mathfrak{p}^*$. Then*

$$\left|H^1(\mathrm{Gal}(F(\mu_{p^\infty})/F), E(F(\mu_{p^\infty}) \otimes_K K_{v_0}))^\Delta\right| \sim (1 - \varphi_E(v_0))(1 - \overline{\varphi_E(v_0)}).$$

The remain part of this section will devote to the proof of this lemma. Note that [15] handled the case where E has good reduction above p. We now assume that E has bad reduction either at $\mathfrak{p}$ or at $\mathfrak{p}^*$. The isomorphism between E and E' over F gives rise to an isomorphism

$$H^1\left(\mathrm{Gal}(F(\mu_{p^\infty})/F), E(F(\mu_{p^\infty}) \otimes_K K_{v_0})\right)^\Delta \xrightarrow{\sim} H^1\left(\mathrm{Gal}(F(\mu_{p^\infty})/F), E'(F(\mu_{p^\infty}) \otimes_K K_{v_0})\right)^\epsilon.$$

We will need Proposition 2 in [15] that for any elliptic curve A over a local field k with good ordinary reduction and let $\widetilde{A}$ denote its reduction over the the residue field κ of k, we have

$$|H^1\left(\mathrm{Gal}(k(\mu_{p^\infty})/k), A(k(\mu_{p^\infty}))\right) = |\widetilde{A}(\kappa)[p^\infty]|.$$

Let $w|v_0$ be a place of F above v_0 and κ_w/κ_{v_0} be the residue fields of F_w and K_{v_0} respectively, we have

$$|E'(\kappa_w)| \sim \left(1 - \varphi_{E'}(v_0)^{[\kappa_w:\kappa_{v_0}]}\right)\left(1 - \overline{\varphi_{E'}(v_0)}^{[\kappa_w:\kappa_{v_0}]}\right).$$

If $w_K = 2$, then F/K is a quadratic extension. If E is ramified at v_0, then F/K is ramified at v_0 and let w be the unique place of F above v_0, we have $\kappa_w = \kappa_{v_0}$ and thus

$$\begin{aligned}\left|H^1\left(\mathrm{Gal}(F(\mu_{p^\infty})/F), E'(F(\mu_{p^\infty})\otimes_K K_{v_0})\right)^\epsilon\right| &= \frac{|H^1\left(\mathrm{Gal}(F_w(\mu_{p^\infty})/F_w), E'(F_w(\mu_{p^\infty}))\right)|}{|H^1\left(\mathrm{Gal}(K_{v_0}(\mu_{p^\infty})/K_{v_0}), E'(K_{v_0}(\mu_{p^\infty}))\right)|} \\ &= \frac{|\widetilde{E'}(\kappa_w)|}{|\widetilde{E'}(\kappa_{v_0})|} = 1.\end{aligned}$$

If E has good reduction at v_0, then F/K is unramified at v_0. If v_0 is split over F, then $F \otimes_K K_{v_0} \cong K_{v_0}^2$ and $\epsilon_{v_0} = 1$. It is easy to see

$$\left|H^1\left(\mathrm{Gal}(F(\mu_{p^\infty})/F), E'(F(\mu_{p^\infty})\otimes_K K_{v_0})\right)^\epsilon\right| \sim (1-\varphi_E(v_0))(1-\overline{\varphi_E(v_0)}).$$

If v_0 is inert in F, let w be the unique prime of F above v_0. Note that $\varphi'_{v_0} = \varphi_{v_0}\epsilon_{v_0}$ and $\epsilon(v_0) = -1$.

$$\begin{aligned}\left|H^1\left(\mathrm{Gal}(F(\mu_{p^\infty})/F), E'(F(\mu_{p^\infty})\otimes_K K_{v_0})\right)^\epsilon\right| &= \frac{|H^1\left(\mathrm{Gal}(F_w(\mu_{p^\infty})/F_w), E'(F_w(\mu_{p^\infty}))\right)|}{|H^1\left(\mathrm{Gal}(K_{v_0}(\mu_{p^\infty})/K_{v_0}), E'(K_{v_0}(\mu_{p^\infty}))\right)|} = \frac{|\widetilde{E'}(\kappa_w)|}{|\widetilde{E'}(\kappa_{v_0})|} \\ &\sim \frac{(1-(\varphi\epsilon)(v_0)^2)(1-\overline{\varphi\epsilon(v_0)}^2)}{(1-(\varphi\epsilon)(v_0))(1-\overline{\varphi\epsilon(v_0)})} = (1-\varphi(v_0))(1-\overline{\varphi(v_0)})\end{aligned}.$$

If $w_K = 4$ or 6, by our assumption, v_0 must be ramified over F and ϵ is non-trivial on its inertia subgroup. The proof is now similar to the previous ramified case.

□

3. ∞-adic and p-adic Gross-Zagier Formulae

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and ϕ its associated newform. Let p be a prime where E is potential good ordinary or potential semi-stable. Let $\alpha : \mathbb{Q}_p^\times \longrightarrow \mathbb{Z}_p^\times$ be the character character contained in the representation $(V_pE)^{ss}$ of $G_{\mathbb{Q}_p}$ such that $\alpha|_{\mathbb{Z}_p^\times}$ is of finite order.

Let $\mathcal{K}$ be an imaginary quadratic field such that $\epsilon(E/\mathcal{K}) = -1$ and p splits in $\mathcal{K}$. Let $\Gamma_{\mathcal{K}}$ be the Galois group of the $\mathbb{Z}_p^2$-extension over $\mathcal{K}$. Recall that [4] there exists a p-adic measure $\mu_{E/\mathcal{K}}$ on $\Gamma_{\mathcal{K}}$ such that for any finite order character χ of $\Gamma_{\mathcal{K}}$

$$\chi(\mu_{E/\mathcal{K}}) = \frac{L^{(p)}(1,\phi,\chi)}{8\pi^2(\phi,\phi)} \cdot \prod_{w|p} Z_w(\chi_w,\psi_w),$$

where (ϕ,ϕ) is the Peterson norm of ϕ:

$$(\phi,\phi) = \iint_{\Gamma_0(N)\backslash\mathcal{H}} |\phi(z)|^2 dxdy, \qquad z = x+iy,$$

and for each prime $w|p$ of $\mathcal{K}$, let $\alpha_w = \alpha \circ \mathrm{N}_{\mathcal{K}_w/\mathbb{Q}_p}$ and $\psi_w = \psi_p \circ \mathrm{Tr}_{\mathcal{K}_w/\mathbb{Q}_p}$, and let φ_w be a uniformizer of $\mathcal{K}_w$, then

$$Z_w(\chi_w,\psi_w) = \begin{cases}(1-\alpha_w\chi_w(\varpi_w)^{-1})(1-\alpha_w\chi_w(\varpi_w)p^{-1})^{-1}, & \text{if } \alpha_w\chi_w \text{ is unramified,}\\ p^n\tau((\alpha_w\chi_w)^{-1},\psi_w), & \text{if } \alpha_w\chi_w \text{ is of conductor } n \geq 1.\end{cases}$$

The following lemma will be used to prove our main theorem.

Lemma 3.1. *Let E be an elliptic curve over $\mathbb{Q}$ with CM by an imaginary quadratic field K. Assume p is also split in K write $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$ with $\mathfrak{p}$ induced by ι_p, i.e. identify $K_\mathfrak{p}$ with $\mathbb{Q}_p$ and the non-trivial element $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ induces an isomorphism on $\mathbb{A}_K$ and thus $\tau : K_{\mathfrak{p}^*} \xrightarrow{\sim} K_\mathfrak{p} = \mathbb{Q}_p$. Let φ be its associated Hecke character. Then we have $\alpha = \varphi_{\mathfrak{p}^*} \circ \tau^{-1}$ and $(\alpha^{-1}\chi_{\mathrm{cyc}})(x) = \varphi_\mathfrak{p}(x)x^{-1}$ for any $x \in \mathbb{Q}_p^\times$. Moreover, for any place $w|p$ of $\mathcal{K}$, any finite order character $\nu : \widehat{\mathbb{Q}}^\times/\mathbb{Q}^\times\widehat{\mathbb{Z}}^{\times(p)}\mathbb{Z}_{p,\mathrm{tor}}^\times \to \mu_{p^\infty}$ viewed as character on Γ_K by compose with norm*

$$Z_w(\alpha_w\nu_w,\psi) = \tau(\varphi_\mathfrak{p}\nu_p^{-1},\psi) \cdot \frac{1-(\varphi_\mathfrak{p}\nu^{-1})(p)p^{-1}}{1-\overline{(\varphi_\mathfrak{p}\nu_p^{-1})}(p)p^{-1}}.$$

Proof. The claim follws from the relations $\varphi\overline{\varphi} = |\ |_{\mathbb{A}_K^{(\infty)}}^{-1}$ and $\varphi^\tau = \overline{\varphi}$.

□

Let $\chi_{\mathrm{cyc},\mathcal{K}} : \Gamma_{\mathcal{K}} \to \mathbb{Z}_p^\times$ denote the p-adic cyclotomic character of $G_{\mathcal{K}}$. Let χ be an anticyclotomic character. Define $\mathscr{L}_{E/\mathcal{K},\chi}$ to be the p-adic L-function

$$\mathscr{L}_{E/\mathcal{K},\chi}(s) = \mu_{E/\mathcal{K}}(\chi\chi_{\mathrm{cyc},\mathcal{K}}^{s-1}), \quad s \in \mathbb{Z}_p.$$

For trivial χ, we write $\mathscr{L}_{E/\mathcal{K}}$ for $\mathscr{L}_{E/\mathcal{K},\chi}$.

Theorem 3.2 (See [19] and [4])**.** *Let E be an elliptic curve over $\mathbb{Q}$ and $\mathcal{K}$ an imaginary quadratic field. Let p be a potentially good ordinary prime for E and split over $\mathcal{K}$. Assume that $\epsilon(E/\mathcal{K}) = -1$. Then*

$$\frac{\mathscr{L}'_{E/\mathcal{K},\chi}(1)}{R_p(E/\mathcal{K},\chi)} \cdot \frac{L_p(E/\mathcal{K},\chi,1)}{\prod_{w|p} Z_w(\chi_w,\psi_w)} = \frac{L'(E/\mathcal{K},\chi,1)}{R_\infty(E/\mathcal{K},\chi)\cdot 8\pi^2(\phi,\phi)}.$$

Here $L_p(E/\mathcal{K},\chi,1)$ is the Euler factor at p. In particular, $\mathscr{L}'_{E/\mathcal{K}}(1) = 0$ if and only if $L'(E/K,1) = 0$.

Proof. Let B be an indefinite quaternion algebra over $\mathbb{Q}$ ramified exactly at the places v of $\mathbb{Q}$ where $\epsilon_v(E/\mathcal{K},\chi)\eta_v(-1) = -1$. It is known that there exists a Shimura curve X over $\mathbb{Q}$ (with suitable level) and a non-constant morphism $f : X \to E$ over $\mathbb{Q}$ mapping a divisor in Hodge class to the identity of E such that its corresponding Heegner cycle $P_\chi(f)$ is non-trivial if and only if $L'(1,\phi,\chi) \neq 0$ by Theorem 1.2 in [19], and if and only if $\mathscr{L}'_{E/\mathcal{K},\chi}(1) \neq 0$ by Theorem B in [4]. Thus $L'(E/\mathcal{K},\chi,1) = 0$ if and only if $\mathscr{L}'_{E/\mathcal{K},\chi}(1) = 0$.

Now assume that $L'(E/\mathcal{K},1) \neq 0$. By an argument of Kolyvagin, we know that $(E(K_\chi)\otimes\mathcal{O}_\chi)^\chi$ is of $\mathcal{O}_\chi$-rank one,

$$\frac{\widehat{h}_\infty(P_\chi(f))}{R_\infty(E/\mathcal{K},\chi)} = \frac{\widehat{h}_p(P_\chi(f))}{R_p(E/\mathcal{K},\chi)} \in \overline{\mathbb{Q}}^\times.$$

By [19] theorem 1.2,

$$\frac{L'(E/\mathcal{K},\chi,1)}{R_\infty(E/\mathcal{K},\chi)\cdot 8\pi^2(\phi,\phi)} = \frac{\widehat{h}_{NT}(P_\chi(f))}{R_\infty(E/\mathcal{K},\chi)} \frac{4L(1,\eta)}{\pi c_{\mathcal{K}}} \frac{L(1,\pi,\mathrm{ad})}{8\pi^3(\phi,\phi)} \alpha^{-1}(f,\chi)$$

and by [4] theorem B (with our definition of $\mathscr{L}_{E/\mathcal{K},\chi}$),

$$\frac{\mathscr{L}'_{E/\mathcal{K},\chi}(1)}{R_p(E/\mathcal{K},\chi)} = \frac{h_p(P_\chi(f))}{R_p(E/\mathcal{K},\chi)} \frac{4L(1,\eta)}{\pi c_{\mathcal{K}}} \frac{\prod_{w|p} Z_w(\chi_w,\psi_w)}{L_p(E/\mathcal{K},\chi,1)} \frac{L(1,\pi,\mathrm{ad})}{8\pi^3(\phi,\phi)} \alpha^{-1}(f,\chi),$$

where the $\alpha(f,\chi) \in \overline{\mathbb{Q}}^\times$. The theorem follows. □

Now we give an explicit form of p-adic Gross-Zagier formula as an application. Let c be the conductor of χ. Assume the following Heegner hypothesis holds:

(1) $(c,N) = 1$, and no prime divisor q of N is inert in $\mathcal{K}$, and also q must be split in $\mathcal{K}$ if $q^2|N$.
(2) $\chi([\mathfrak{q}]) \neq a_q$ for any prime $q|(N,D)$, where $\mathfrak{q}$ is the unique prime ideal of $\mathcal{O}_{\mathcal{K}}$ above q and $[\mathfrak{q}]$ is its class in $\mathrm{Pic}(\mathcal{O}_c)$.

Let $X_0(N)$ be the modular curve over $\mathbb{Q}$, whose $\mathbb{C}$-points parametrize isogenies $E_1 \to E_2$ between elliptic curves over $\mathbb{C}$ whose kernel is cyclic of order N. By the Heegner condition, there exists a proper ideal $\mathcal{N}$ of $\mathcal{O}_c$ such that $\mathcal{O}_c/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. For any proper ideal $\mathfrak{a}$ of $\mathcal{O}_c$, let $P_{\mathfrak{a}} \in X_0(N)$ be the point representing the isogeny $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}$, which is defined over the ring class field H_c over $\mathcal{K}$ of conductor c, and only depends on the class of $\mathfrak{a}$ in $\mathrm{Pic}(\mathcal{O}_c)$. Let $J_0(N)$ be the Jacobian of $X_0(N)$. Let $f : X_0(N) \to E$ be a modular parametrization mapping the cusp ∞ at infinity to the identity $O \in E$. Denote by $\deg f$ the degree of the morphism f. Define the Heegner divisor to be

$$P_\chi(f) := \sum_{[\mathfrak{a}]\in\mathrm{Pic}(\mathcal{O}_c)} f(P_{\mathfrak{a}}) \otimes \chi([\mathfrak{a}]) \in E(H_c)_{\overline{\mathbb{Q}}}.$$

Theorem 3.3. *Let E,χ be as above satisfying the Heegner conditions (1) and (2). Then*

$$L'(1,E,\chi) = 2^{-\mu(N,D)} \cdot \frac{8\pi^2(\phi,\phi)_{\Gamma_0(N)}}{u^2\sqrt{|Dc^2|}} \cdot \frac{\widehat{h}_\infty(P_\chi(f))}{\deg f},$$

where $\mu(N,D)$ is the number of prime factors of the greatest common divisor of N and D, $u = [\mathcal{O}_c^\times : \mathbb{Z}^\times]$ is half of the number of roots of unity in $\mathcal{O}_c$, and $\widehat{h}_\infty$ is the Néron -Tate height on E over $\mathcal{K}$.

Moreover, let p be a prime split in $\mathcal{K}$ and assume that E is potential ordinary at p (i.e. either potential good ordinary or potential semistable), then we have

$$\mathscr{L}'_{E/\mathcal{K},\chi}(1) = \frac{\prod_{w|p} Z_w(\chi_w, \psi_w)}{L_p(E/\mathcal{K},\chi,1)} \cdot \frac{2^{-\mu(N,D)}}{u^2\sqrt{|Dc^2|}} \cdot \frac{\widehat{h}_p(P_\chi(f))}{\deg f},$$

where $\widehat{h}_p$ is the p-adic height on E over $\mathcal{K}$.

Proof. The explicit form of Gross-Zagier formula is proved in [2]. The explicit form of p-adic Gross-Zagier formula then follows from the relation in Theorem 4.1. □

4. Proof of Main Theorem 1.1

In this section, let E be an elliptic curve over $\mathbb{Q}$ with CM by K and Ω_E the minimal real period of E over $\mathbb{Q}$. Let $p \nmid w_K$ be a prime split both in K.

Lemma 4.1. *Let $\mathcal{K}$ be an imaginary quadratic field where p splits, η the associated quadratic character, and η_K its base change to K. Assume that $\epsilon(E/\mathcal{K}) = -1$. Then there exists a p-adic unit u such that*

$$\mathscr{L}_{E/\mathcal{K}} = \frac{\tau(\varphi_\mathfrak{p},\psi_\mathfrak{p})^2\cdot\Omega_E^2}{8\pi^2(\phi,\phi)}\cdot\mathscr{L}_\varphi\mathscr{L}_{\varphi\eta_K}.$$

Proof. It's enough to show that for any finite order character $\nu : \widehat{\mathbb{Q}}/\mathbb{Q}^\times\widehat{\mathbb{Z}}^{\times(p)}\mathbb{Z}_{p,\mathrm{tor}}^\times \to \mathbb{C}^\times$, we have

$$\nu_\mathcal{K}(\mu_{E/K}) = \tau^2(\varphi_p,\psi_p)\frac{\Omega_E^2}{8\pi^2(\phi,\phi)}\mu_{\mathfrak{f}_0}(\varphi\nu_K^{-1})\mu_{\mathfrak{f}_0}(\varphi\eta_K\nu_K^{-1}).$$

Here $\nu_\mathcal{K} = \nu\circ \mathrm{N}_{\mathcal{K}/\mathbb{Q}}$ and $\nu_K = \nu\circ\mathrm{N}_{K/\mathbb{Q}}$. By interpolation property, the left hand of the formula in the lemma is

$$\frac{L^{(p)}(1,\phi,\nu_\mathcal{K}^{-1})}{8\pi^2(\phi,\phi)}\prod_{w|p}Z_w(\alpha_w\nu_w,\psi_w),$$

Note that $\mathcal{K}/\mathbb{Q}$ splits at p and then η_p is trivial, the right hand side of the formula in the lemma is

$$\frac{\tau(\varphi_\mathfrak{p}\nu_\mathfrak{p}^{-1},\psi_\mathfrak{p})^2}{\tau(\varphi_\mathfrak{p},\psi)^2}\cdot\left(\frac{1-\varphi\nu^{-1}(\mathfrak{p})p^{-1}}{1-\overline{\varphi\nu^{-1}}(\mathfrak{p})p^{-1}}\right)^2\cdot\frac{L^{(p\mathfrak{f}_0)}(\overline{\varphi\nu^{-1}},1)}{\Omega}\cdot\frac{L^{(p\mathfrak{f}_0)}(\overline{\varphi\nu^{-1}\eta_K},1)}{\Omega}$$

Then the formula follows from lemma 3.1. □

We are ready to prove Theorem 1.1. Assume that $L(s,E/\mathbb{Q})$ has a simple zero at $s=1$ and that p is a bad but potentially good ordinary prime for E. Let φ be the Hecke character associated to E and $\mathfrak{f}_0$ its the prime-to-p conductor. We may choose an imaginary quadratic field $\mathcal{K}$ such that

- $L(s,E/\mathcal{K})$ also has a simple zero at $s=1$.
- p is splits in $\mathcal{K}$.
- the discriminant of $\mathcal{K}$ is prime to $\mathfrak{f}_0$.

Note that related Euler factors are trivial in this case, we then have

- $\mathscr{L}_{\varphi\eta_K}(1) = \dfrac{L(1,E^{(\mathcal{K})})}{\Omega_{E/K}}$,
- $\dfrac{\mathscr{L}'_{E/\mathcal{K}}(1)}{R_p(E/\mathcal{K})\tau(\varphi_\mathfrak{p},\psi_\mathfrak{p})^2} = \dfrac{L'(E/\mathcal{K},1)}{R_\infty(E/\mathcal{K})8\pi^2(\phi,\phi)}$.
- $\mathrm{ord}_p(|\text{Ш}(E/\mathbb{Q})|) = \mathrm{ord}_p\left(\dfrac{\mathscr{L}'_\varphi(1)}{R_p(E/\mathbb{Q})}\right)$,
- $\mathrm{ord}_p\left(\dfrac{\mathscr{L}'_{E/K}(1)}{\mathscr{L}'_\varphi(1)\mathscr{L}_{\varphi\eta_K}(1)}\right) = \mathrm{ord}_p\left(\dfrac{\tau(\varphi_\mathfrak{p},\psi_\mathfrak{p})^2\Omega_{E/K}^2}{8\pi^2(\phi,\phi)}\right)$,
- $\mathrm{ord}_p\left(\dfrac{\Omega_{E/K}}{\Omega_E}\right) = \mathrm{ord}_p\left(\dfrac{R_p(E/\mathcal{K})}{R_p(E/\mathbb{Q})}\right) = 0.$

It follows that

$$\mathrm{ord}_p(|\text{Ш}(E/\mathbb{Q}|)) = \mathrm{ord}_p\left(\frac{L'(E/\mathbb{Q},1)}{\Omega_E\cdot R_\infty(E/\mathbb{Q})}\right).$$

This proves Theorem 1.1 (i). Assume that $E(\mathbb{Q})$ has rank one and $\text{Ш}(E/\mathbb{Q})(p)$ is finite, or equivalently, $E(K)$ has $\mathcal{O}_K$-rank one and $\text{Ш}(E/K)$ is finite. By [1], the cyclotomic p-adic height pairing is non-degenerate. Thus both $\mathscr{L}_{\varphi_E}$ and $\mathscr{L}_{\overline{\varphi_E}}$ have exactly order 1 at $s=1$, therefore $\mathscr{L}_{E/\mathcal{K}}$ has exactly order

one at $s = 1$. It follows from p-adic Gross-Zagier formula that the related Heegner point is non-trivial and therefore $L(E, s)$ has a simple zero at $s = 1$. This completes the proof of Theorem 1.1.

References

[1] Daniel Bertrand, *Propriétés Arithmétiques de Fonctions Thêta à plusieurs variables*, Lect. Notes in Math., vol 1068, pp. 17-22. Berlin-Heidelberg-New York-Tokyo: Springer 1984.

[2] L. Cai, J. Shu and Y. Tian, *Explicit Gross-Zagier and Waldspurger formulae.* Algebra Number Theory 8 (2014), no. 10, 2523-2572.

[3] J.Coates and A.Wiles, *On p-adic L-functions and elliptic units.* J. Austral. Math. Soc. Ser. A 26 (1978), no. 1, 1-25.

[4] Daniel Diegni, The p-adic Gross Zagier formula on Shimura curves, Preprint.

[5] E.de Shalit, *The Iwasawa theory of elliptic curves with complex multiplication*, Perspect. Math. Vol.3 (1987).

[6] G. Faltings, *Crystalline cohomology and p-adic Galois-representations.* Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988), Johns Hopkins Univ. Press, Baltimore, MD, 1989.

[7] S. Friedberg and J. Hoffstein, *Nonvanishing theorems for automorphic L-functions on GL(2).* Ann. of Math. (2) 142 (1995), no. 2, 385-423.

[8] Kobayashi, Shinichi, *The p-adic Gross-Zagier formula for elliptic curves at supersingular primes.* Invent. Math. 191 (2013), no. 3, 527 -629.

[9] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer.* Invent. Math. (1986) Volume 84, no. 1, pp 1-48.

[10] B,Perrin-Riou, *Groupe de Selmer d'une courbe elliptique multiplication complexe*, Compositio Math. 43 (1981), no. 3, 387-417.

[11] B. Perrin-Riou, *Descente infinie et hauteur p-adique sur les courbes elliptiques multiplication complexe*, Invent. Math. 70 (1982/83), no. 3, 369-398.

[12] B. Perrin-Riou, *Points de Heegner et dérivées de fonctions L p-adiques*, Invent. Math. 89 (1987), no. 3, pp. 455-510.

[13] K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. 89 (1987), no. 3, 527-559.

[14] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 103 (1991), no. 1, 25-68.

[15] P.Schneider, *Iwasawa L -functions of varieties over algebraic number fields. A first approach*, Invent. Math. 71 (1983), no. 2, 251-293

[16] Y. Tian, *Congruent Numbers and Heegner Points*, Cambridge J. of Math, Vol. 2.1. 117-161, 2014.

[17] Y. Tian, X. Yuan and S. Zhang, *Genus Periods, Genus Points and Congruent Number Problem*, to appear in Asian Journal of Mathematics.

[18] R.Yager, *On two variable p-adic L-functions*, Ann. of Math. (2) 115 (1982), no. 2, 411-449.

[19] X.Yuan, S. Zhang, and W. Zhang, *The Gross-Zagier Formula on Shimura Curves*, Annals of Mathematics Studies Number 184, 2013.